The Claims

Claims 1-6 (Canceled).

7. (Previously presented) A system supporting public key encryption, the system comprising:

a certifying authority;

a client device, coupled to the certifying authority, to,

generate a blinded certificate including a public key, and

transmit the blinded certificate to the certifying authority;

wherein the certifying authority is to digitally sign the blinded certificate and encode security attributes of the client device into the digital signature;

wherein the certifying authority is to digitally sign the blinded certificate according to a formula

$$(\text{blinded certificate})^{d} \bmod (n),$$

wherein d represents a private key of the certifying authority and wherein n is a product of two prime numbers that comprise the private key; and

wherein the certifying authority is to encode a security attribute into the digital signature by:

representing the security attributes as a series of bits;

identifying, for each bit in the series that has a particular value, a corresponding integer; and

generating as the value d the product of the identified integers.

8. (Original) A system as recited in claim 7, wherein the certifying authority is further to generate another digital signature for the blinded certificate by:

additionally identifying, for each bit in the series that has another value, a corresponding integer; and

generating as the value *d* for the other digital signature the product of the additionally identified integers.

Claims 9-14 (Canceled).

15. (Previously presented) A method comprising:

receiving, from a client, a current certificate and a request to sign a new certificate;

determining attributes of the client based on the current certificate;

selecting, in accordance with public key cryptography, a public/private key pair that is based at least in part on the attributes of the client;

digitally signing the new certificate using the selected private key;

wherein the digitally signing comprises calculating a value of a formula

$$(\text{blinded certificate})^d \bmod (n),$$

wherein *d* represents a private key of a device performing the digital signing and wherein *n* is a product of two prime numbers that comprise the private key; and

wherein the selecting comprises:

representing the attributes as a series of bits;

identifying, for each bit in the series that has a particular value, a corresponding integer; and

generating as the value *d* the product of the identified integers.

16. (Original) A method as recited in claim 15, further comprising generating another digital signature for the blinded certificate by:

additionally identifying, for each bit in the series that has another value, a corresponding integer; and

generating as the value *d* for the other digital signature the product of the additionally identified integers.

Claims 17-24 (Canceled).

25. (Previously presented) A method comprising:

receiving, from a client, a request for electronic content;

checking, based on information encoded in a digital signature of at least a portion of the request, whether the client has a set of claimed security attributes;

determining how to respond to the request based on the checking;

wherein the checking comprises:

representing the set of claimed security attributes as a series of bits;

generating a public key for a certifying authority using the series of bits; and

using the public key to verify the digital signature; and

wherein the generating comprises:

identifying, for each bit in the series that has a particular value, a corresponding integer; and

generating as the public key the product of the identified integers.

Claims 26-34 (Canceled).

35. (Currently amended) One or more computer-readable media containing a plurality of instructions that, when executed by one or more processors, causes the one or more processors to:

receive, from a client, a request for electronic content;

check, based on information encoded in a digital signature of at least a portion of the request, whether the client has a set of claimed security attributes by determining a public key based on the set of claimed security attributes and using the public key to verify the digital signature; and

determine how to respond to the request based on the checking;

wherein the instructions that cause the one or more processors to check whether the client has a set of claimed security attributes further cause the one or more processors to represent the set of claimed security attributes as a series of bits and generate the public key using the series of bits;

wherein the instructions that cause the one or more processors to generate the public key further cause the one or more processors to:

identify, for each bit in the series that has a particular value, a corresponding integer; and

generate as the public key the product of the identified integers.

Claims 36-37 (Canceled).